



# THE NEW FEDERAL CTO

## Short White Paper by Sun Microsystems

### DRAFT

#### **1. The Publicly Stated Mission.**

*"Bring Government into the 21st Century: Use technology to reform government and improve the exchange of information between the federal government and citizens while ensuring the security of our networks. Appoint the nation's first Chief Technology Officer (CTO) to ensure the safety of our networks and lead an interagency effort, working with chief technology and chief information officers of each of the federal agencies, to ensure that they use best-in-class technologies and share best practices."*

[http://change.gov/agenda/technology\\_agenda/](http://change.gov/agenda/technology_agenda/)

The Obama campaign's Technology Plan went further, by adding the following taskings to the CTO --

- *"The CTO will have a specific focus on transparency, by ensuring that each arm of the federal government makes its records open and accessible as the E-Government Act requires. The CTO will also focus on using new technologies to solicit and receive information back from citizens to improve the functioning of democratic government."*
- *"The CTO will also ensure technological interoperability of key government functions. For example, the Chief Technology Officer will oversee the development of a national, interoperable wireless network for local, state and federal first responders as the 9/11 commission recommended."*

The Plan also announced that technology and innovation would be leveraged by the Administration to help: (1) create a new level of transparency, accountability and participation for America's citizens in the federal government; (2) lower health care costs; (3) solve critical energy and environmental problems; (4) upgrade education; and (5) modernize public safety networks.

#### **2. Sun's Position.**

We support the publicly stated mission. It represents a policy injection on how the processes of government, fueled by technology, can change.

We believe such dynamic change will require commensurate change to the Federal Government's IT organization, culture and purchasing practices. This would include:

##### **The creation of a Federal CIO.**

- The publicly stated mission is consistent with a CIO's duties.
- The President needs an operational champion who is inwards-facing, focused on enabling the Federal Government's own systems and transformation.
- The OSTP Director can take on the role of the externally-facing tech leader. Essentially, this would enable both a CIO and a CTO that report to the President – which is common in the private sector.
- With a \$100 billion spend for IT products and services, there was already need for such a federal government position; this need is exacerbated by the transformational goals of the President-elect.

##### **The empowerment of the new Federal CIO.**

Having an empowered CIO would enable government-wide IT transformation of how the government does its business. Not having such a central, empowered CIO to guide the federal agencies in a common



direction, with performance metrics and means to reward attainment of those metrics, has held back and increased the cost of IT within the federal government.

- The Federal CIO should be cabinet level, certainly a direct report to the President.
- The Federal CIO must be able to enforce compliance. Compliance is enabled by organizational stature and by impacting purse strings. The Federal CIO should have budget authority on agency IT plans and spends, with the ability to reward those agency CIOs meeting mission objectives.
- “If it touches the network, then the CIO has veto power over it.” Political aircover is supplied by the President.
- Control over policy and budget oversight should be centralized with the Federal CIO; execution should be decentralized to the agency CIOs. Audit and metric functions should be used to measure compliance, budget control should be used to enforce compliance.
- To drive interoperability between and among government agencies, and to the citizens they serve, the Federal CIO must have a clear mandate to drive ICT standards – and to project those standards (surrounding neutral, royalty free representations of all government information) into the nation's digital networks.
  - Such interoperability is vital to national security, as well as to the President-elect's technology, innovation, health care, and environmental agendas.
- Key technology horizontals (including interoperability) should be controlled by the Federal CIO.
- The CIO should refrain from unfunded mandates and budget reallocations to fund mandates.
- Agency CIO appointments should require, at minimum, approval by the Federal CIO. Consider actually having the Federal CIO as lead, with approval by the respective agency head.
- Agency CIOs should have dual reporting lines. Consider having the solid line to the Federal CIO, with the dotted line to the agency head.

#### **Concentration by the new Federal CIO on core deliverables.**

- The Federal CIO shall articulate the problems his/her office will solve for the other cabinet offices.
- The publicly stated mission relies on core policy concepts, to be enforced across the federal government – (1) transparency; (2) collaboration and interoperability; (3) cyber security and safety, with privacy enabled; (4) citizen access, participation, and empowerment; and (5) energy efficiency and green IT.
- These core policy concepts require horizontal technology architectures enforced across the federal government. These horizontals should include: (1) identity management; (2) interoperability and open standards; (3) open source software; (4) cloud computing, and (5) thin clients.
- Interoperability will not be easily achieved – the nation's current standards development infrastructure has struggled to develop timely, global, interoperable ICT standards, much less the suites of closely integrated standards that will be needed to solve the complex problems raised by the publicly stated mission. For more, see <http://www.consortiuminfo.org/bulletins/oct08.php#policy>.
  - Just as one example, cloud computing environments should have open standards interfaces so that the Federal Government is not locked into any one cloud computing solution or supplier.
- Accomplishing these deliverables will include embracing Web 2.0 technologies, promoting the use of open formats and search-accessible websites, and encouraging innovative uses of new technology platforms. ([http://www.readwriteweb.com/archives/millennials\\_route\\_around\\_it\\_departments.php](http://www.readwriteweb.com/archives/millennials_route_around_it_departments.php))
- The Federal CIO should change IT acquisition, contract, and program management process to incentivize reuse. Today's policies incentivize the System Integrators (SIs) and Government Organizations to rebuild the same functions/systems over and over again. This leads to great expense and a huge waist of the taxpayer's money. It also creates systems that do not integrate and do not



allow the effective sharing of information along with lack of services for the warfighter and US Citizens. Program managers and System Integrators should have a financial incentive to build things are that generalized enough for reuse, get a financial incentive when other organizations reuse their system or component, and get a financial incentive when they reuse others systems or components. This will naturally push the whole Federal Government IT environment towards integrated solutions, rather than the current acquisition and contracting system that has the opposite effect.

- The Federal CIO would “pull from across the federal sphere” the projects and best practices that are being applied in one agency and could be learned from/applied in others.
- As part of citizen access and empowerment, the Federal CIO should focus on persons with disabilities -- see <http://projects.gnome.org/accessibility/screencasts.html> and <http://www.aegis-project.eu/>.

### **An enabling organizational structure for the Federal CIOs office.**

- The CIO should be a political appointee with both the President and his cabinet.
- To facilitate knowledge of the government and communication with the agency personnel, a career deputy could be appointed.
- If central service organizations are created, this office should ensure they have competitive pressures based on SLA (Service Level Agreements) to ensure both good service and competitive costs/operations/chargebacks.
- The CIO office would be focused on oversight, budget, and execution of cross fictional initiatives. It would have budget control, but not be operational. There would need to be a core staff, then representatives from every CIO organization within the Federal Government.
- Organization should be based on Industry standards such as: COBIT – governance and structure; ITIL – operations/infrastructure; CMMI – Process and control/Metrics; PM certifications (Prince 2 or equivalent) – Program management; and Six Sigma – Change acceleration and quality control.
- An ideal example CIO office would include the following parts, with the first five consistent with project flow/lifecycle:

#### Oversight and Management:

- **User Advocacy** – An end users advocate focuses on user and citizen productivity. Each agency/business unit focuses only on the delivery/automation of their services, whereas the user advocate focuses on the experience and productivity of a government employee and a citizen interfacing with the systems from an end-to-end perspective
- **CISO** – Chief Information Security Officer – lead for cyber security.
- **IT Governance** – Handles and creates IT policy and manages the enforcement and compliance to policy.
- **Contracts and Vendor Management** – oversight of acquisition policies related to IT across the federal government. Also has the power to push back against power lobbyists that tend to disrupt the growth of open standards and integrated solutions.
- **IT communications** – This is a very important for change management and user acceptance as the CIO transforms the government. Very few issues are technical, most are related to people. This organization along with the User Advocate would work on change management and deal with the press.

#### Delivery:

- **IT CTO** – looks ahead at emerging technologies and opportunities. (focuses on Government internal IT)
- **Strategy and Architecture** – creates the blueprints of the current, and things to come. Sets open standards for all cross functional initiatives, not products. Has Architecture



representatives from the agencies/business units that contribute to cross functional shared initiatives.

- **Business and Infrastructure Systems** – uses the blueprints developed by the Architecture organization to engage the business units/agencies and build the systems. Has functional experts/representatives that advocate for the agencies.
- **Systems Engineering Process Group** – makes sure the systems have consistent quality assurance and meets the standards set by the Strategy and Architecture team. Defines the processes to be followed and puts metrics and controls in place. Defines and maintains standards to be used in development and deployment (for example programming standards).
- **IT Operations** – oversees the operation of the systems and the IT infrastructure (networks, clouds, data centers, help desk and desktops) and supports the business units / agencies. Has operational representatives from the agencies / business units.
  
- **The ideal CIO should be an individual that has extensive experience in the following areas:**
  - Practical application and work in real world situations as a CIO is more important than educational background.
    - Success here is not academic, this person needs “hands on” experience as a CIO.
    - Success here is not about being an industry “visionary”, its much more about a track record of getting things done in large organizations.
    - Should have worked as a CIO of a Fortune 500 company.
  - Should have experience in the Federal CIO ranks, either as an SES level CIO or CTO, or in a CIO staff position. It is very important that they can navigate large government organizations as well as experience with large commercial IT organizations and budgets.
  - Should have championed open standards, interoperability, consolidation, and transforming the business with information technology.
  - Must have had a service focus rather than an entitlement focus.
  - Should have experience in the three major areas of IT before becoming a CIO: Operations, Application development, and Architecture.
  - Should be focused on managing with metrics and have a strong process background.
  - The ideal candidate would also have had some experience working in an IT organization of a start-up, so they also understand the vultures and pitfalls of working in that environment, and they can apply those learnings to large organizations and projects.
  - The ideal candidate should also have some experience working on the business side, either leading a business unit as a general manager in a Fortune 500 company, or leading a functional organization within the Federal Government.
    - Its important that the CIO has a good understanding of the functional side of the business (not having a background only in information technology).



## Supporting data points

### **3. Supporting data points -- Open source and open standards.**

According to the IDC Group, open source software (OSS) is “the most significant all-encompassing and long-term trend that the software industry has seen since the early 1980s.” Gartner projects that by 2012, 90 per cent of the world’s companies will be using open source software. Indeed, try to name a successful 21<sup>st</sup> century IT startup that hasn’t relied on OSS. Great progress is also being made by governments in Latin America, Europe, and Asia in more efficiently and effectively serving their citizens -- and reducing the digital divide -- by leveraging OSS.

Open source software has been more extensively used in the US military and intelligence agencies in the last 10 years, primarily because of its security advantages. The NHIN initiative at HHS is leveraging open source software across multiple agencies, especially within the NHIN-Connect, wherein a production ready gateway to exchange electronic health data has been successfully demonstrated between federal agencies. This open-source gateway will go into production in January, and the source code will be released to the community in March. It is estimated that if this pilot had instead used proprietary software, \$200+ million in software licenses would have been necessary, and the procurement process would have delayed the pilot for at least another two years.

A draft Guidance Memo is pending in the DOD CIO's office that will provide further impetus to OSS use in the federal government. This draft memo reportedly cites seven OSS advantages to be considered as factors when selecting software products (with particular focus on security). They sound very similar to advantages that Sun has been citing for some time now as concerns open source and open standards:

**Lower barriers to entry.** Open source is free to download. No licensing fees. Open source and open standards allow multiple vendors to compete fairly over implementation – enabling more capitalist competition, not less. Such competition brings more choices, better products, and lower prices. Indeed, open source should be considered an extension of long established COTS policies within the government. Those policies are aimed at gaining the advantages of commercial best practices.

Open source also improves the procurement cycle by allowing “test drives” before RFP. Requirements gathering, system development and testing can be virtually complete before a procurement has to run, and without vendor lock-in. This has been important to both Navy CANES and HHS NHIN-Connect. In addition, open source increases speed and flexibility by allowing expansions and changes to occur without going through a slow and complex procurement process.

**More security.** It has been established that OSS tends to be more secure than the equivalent proprietary products. This is because, just like what has been established in cryptography (i.e., RSA vs Clipper Chip), public and community exposure strengthens the code and ensures there are no secrets in the code that can be exploited. Security through obscurity, isn't.

- Open development means the security secret can't be in the code, it must be managed outside the code.
- At a recent AFCEA conference the Director of the NSA confirmed that the NSA has found that open source code provides better cyber security than proprietary code;
- Statistics pulled from the National Vulnerability Database confirm that OSS products have had significantly less vulnerabilities exploited than the equivalent proprietary products. Products like



Java, Solaris, MySQL, and Mozilla have a proven record of less security issues throughout their life cycle than comparable proprietary products.

- Moreover, the ability for the government to engage in a community process to modify source code enables timely response to changing situations and threats. If needed, government can make security adjustments on its own time frame, and not the vendor's.

**Increased interoperability.** Open source and open standards are the fastest route to interoperability, as the code, APIs, and interfaces are published for all to see. Its easier for others, including competitors, to write interoperable apps, platforms, etc. Open source is a key component of the DOD strategy to achieve data interoperability across applications. Open source now works on all platforms used by the federal government.

**More R&D bang for the buck.** Millions of developers around the globe work on open source projects. They come from a large number of companies, from vendors to end users, that are using open source to advance their business. That way, by using open source software, the federal government becomes part of a large community that is investing resources to improve the software.

**Citizen, supplier, and partner access.** Too often, citizens, suppliers, and partners are discriminated against by proprietary software restrictions. Governments globally are realizing they've lost control over and access to their own documents and records. Open formats, open source, and open standards should be a component of driving towards more open, and accessible, government now and into the future.

**Lower barriers to exit.** Public code means support can be provided by multiple vendors and systems integrators. If a vender EOSL, others can step in. The government is provided investment protection beyond any single vendor. Also, continual innovation means technology can have a short shelf life, and governments (and their taxpayers) shouldn't be reliant on a vendor who knows the customer is too locked-into their solution to switch.

In sum, OSS increases competition and innovation among vendors, reduces the cost of deployment, speeds deployment, saves taxpayer dollars, and improves the overall cyber security of the Federal Government information technology environment. What horizontal policies should the Obama Administration adopt in this area? Sun makes the following recommendations.

**Procurement.** Formally allow and leverage the use of open source where benefits can be expected:

- Facilitate and provide incentives for reuse, collaboration, and donation of code to the community;
- List open standards and open source as priority criteria in determining best value and performance, and in determining full and open competition compliance;
- Require procurers have a strong differentiated reason to spend the extra money and risk the legacy lock-in of a proprietary product selection; and
- Include the cost of having to exit a proprietary product and move to another in evaluating full cost of ownership.

**Licensing.** For a product to be open source, it must be licensed under an OSI approved license. There are about 40 different licenses available at <http://www.opensource.org/> If a product is not distributed under an OSI license, then it is not open source. Other scenarios to consider include when:

- The vendor has provided a written commitment to open source the product under one of these



- licenses in a specific time frame and the vendor has a proven track record of open sourcing products.
- Distributions that are largely based on, or derivatives of, open source products should make the source code available to any user at no cost, and the full production binary should be available for unsupported use at no cost.

### **Support and Protection.**

- Real 24x7 enterprise level support should be available, to ensure that the procurer can get mission critical support when needed.
- Vendors should be able and willing to indemnify their own products, including the products' open source content, so that the procurer or user will not incur unfair costs from patent trolls or other aggressive parties based on intellectual property issues.
- Vendors shall have made strong and clear promises to use their IP rights only defensively with respect to the products, and when they are members of standards bodies also not to use their IP rights offensively against implementers of the standards they're promoting, even other vendors.

**Communities.** The federal government should encourage and join open source and open standards communities.

- Interfaces to products should be managed by an open standards body (e.g., W3C, OASIS, IETF, Liberty Alliance) wherever possible to facilitate interoperability with other products. Document and other formats shall be maintained in an open standards body, be freely available to vendors, and have been implemented in multiple applications.
- When appropriate (e.g., in the government's own interests), governments should release code advancements back to the public under an OSI-approved open source license.

**Non-Discriminatory and Improved Access.** Citizens, suppliers, and partners should have non-discriminatory access to government websites, electronic services, forms, and documents. The Norwegian government has accomplished this by requiring the use of open formats as follows: HTML for publishing public information on the internet; PDF for documents that need to maintain their original appearance; and ODF to publish documents which the user may need to download and fill out. Websites must be browser agnostic.

- Procurement policy should encourage open formats, so that the government retains access to and control over electronic documents and records without discriminatory reliance on the software application on which the documents or records were first created. ODF should be considered as the default format for editable documents. (ODF is already supported by over 50 proprietary and open source applications, and Microsoft is committed to its support in 2009.)
- Procurement policy and research grants should encourage the development of affordable, productivity-enhancing IT solutions for persons with disabilities, leveraging open source software.

### **4. Supporting data points – Data Center Energy Efficiency.**

It is estimated that the average data center burns through 2 tons of coal an hour. The EPA estimated in 2007 that under current efficiency trends, national energy consumption by servers and data centers could nearly double again in another five years to more than 100 billion kWh, representing a \$7.4 billion annual electricity cost.

- IDC has estimated that for every \$1 spent on new IT hardware, an additional \$0.50 is spent on power and cooling. More than double the amount 5 years ago.
- Gartner estimates 70 percent of CIOs are reporting that power and/or cooling issues are now their single largest problem in the data center. Uptime Institute says 42 percent of data centers managers



believe they will run out of power capacity in the next 12-24 months.

We think these numbers are indicative also of what is happening in the Federal Government. It may actually understate it, as federal CIOs are normally not accountable for data center energy use, and therefore are not taking active steps to address it.

Sun decided to take on this problem internally, with focus on two of our own data centers. The results:

- Reduced energy use by 1.5 megawatts (MW), floor space by 88%, CO<sub>2</sub> emissions by 3,227 tons, and costs by \$9 million.
- One datacenter now has a Data Center Infrastructure Efficiency (DCiE) rating of 78%, compared with an industry average of approximately 50%. These efficiencies are leading to additional savings of \$400,000 per year at this data center.

The Federal CIO should address this issue by incenting agency CIOs to be energy efficient. They should be explicitly accountable for the energy costs of their IT systems, and eligible to realize the savings brought about through increased efficiencies. This may require an amendment to Clinger-Cohen.

### **5. Supporting data points -- Thin Client Architecture.**

Primarily for security and cost reasons, the intelligence and military agencies have been moving recently to stateless thin clients. There are large deployments at DIA, JICPAC, SPAWAR, US Army Intelligence (where General Custer has 6,000 thin clients powering 160 classrooms with only 2 admins, saving \$31.5m over the past year), Los Alamos National Labs, DOE, and US Navy Integrated Warfare Systems Lab.

The advantages are: increased cyber security, reduced costs, and eco responsibility.

#### **Increased Cyber security.**

- All the content is protected back in the server room. If a Stateless Thin Client is stolen or lost, there is no panic over whether there was sensitive data on the client, and if there was, who must be notified and what liabilities have been potentially exposed. Because no data could have been on the client. Its just like if your flat screen TV were stolen. You lost the TV, nothing more.
- There are no operating systems on the client to manage. Meaning no viruses.
- Zero data for work from home and remote users, so telecommuting and remote work can be facilitated without the normal, significant risk of government data being lost, stolen, or broken.
- High security via built in Ipsec tunnel for the client with its own SIM chip, device and firmware authentication, two (or three) factor JavaBadge user authentication and encryption in addition to the device Ipsec.
- Access and authorities are controlled and audited back on the server, so employees and contractors access can be immediately and accurately amended as appropriate, and a robust audit trail maintained. Persons who should no longer have access, don't.
- Security personnel can focus on the server room, and closely monitor activity and attempted infiltrations and exfiltrations there, rather than trying to watch thousands of desktops.
- Personnel can implement patches and security upgrades back in the server room, reliably, and quickly.
- Attempted downloads to a server can be blocked and more easily controlled by IT staff.

#### **Reduced costs.**

- On a well designed deployment, you can have one system administrator for every 3K stateless thin clients. (Sun saves about \$12 million a year in desktop administration costs. Don't expect service



- contractors to like this feature.)
- Zero moves, adds, and changes. People move with their JavaBadge, their desktop moves with them. (Sun saves about \$5 million a year on this.)
  - Zero desktop refresh. Expected lifespan of a device is 12 years, as opposed to 2-3 years for a desktop. (Sun saves about \$5 million a year on this.)
  - Clients can be thousands of miles from the server, working fine over managed and unmanaged Internet connections. Can run over the WAN and over standard broadband – Cable DSL, 3G/4G cell, and 802.11. (Many of Sun's offices between 100-200 people only need cable and DSL modems.)
  - Sun can put a new OS out on every stateless thin client in three hours globally, at a total testing/labor cost of about \$50K. That used to take 6-8 months and cost about \$3-5M.
  - If a client breaks, unskilled staff can plug in a new one with no data loss nor service interruption.
  - Compare with PCs -- volume cost of stateless thin client (GSA price \$190, list \$240), server per user cost of about \$37, thin client runs over existing networks, and storage cost of about \$12 a Gig per user for a NAS device.
  - Network loads usually go down after a deployment, because the most common application is email, and on PCs the attachments all have to be shipped across the network to the client. On stateless thin clients, the attachment moves across the data center and is only displayed to the end user.
  - Because desktop utilization is small (less than 1% on a 24x7), Sun is able to run other HPC processes on our Grid when users are not in session. (This could be big savings for many government users, but Sun has not estimated our own savings yet.)
  - Sun has a hub and spoke architecture, with “nothing but network” offices. We replicate user data from one grid center to another, so that if we lose a grid center, no data is lost. We do ZERO remote office backups, and don't need a DR plan for remote offices because there is no data there.
  - Sun relies on stateless thin clients for its employee “open work” telecommuting program. This program saves us about \$68 million a year in real estate costs.

**Eco Responsibility.**

- Each PC uses about 100 Watts. A stateless thin client uses 4.
- Stateless thin clients produce little to no heat.
- The raw materials for 1 PC can make 50 stateless thin clients.
- Expected life time of about 12 years, as opposed to 2-3 years for a PC, meaning less landfill impacts. When recycled or disposed of, there are no hazardous materials involved. There are potentially huge carbon savings by avoiding the PC upgrade cycle and associated manufacturing impact.
- Sun relies on stateless thin clients for its employee “open work” telecommuting program. This program has reduced Sun's CO2 from employee commuting by almost 30,000 metric tons per year.